ELSEVIER

Linear Algebra and its Applications 297 (1999) 9–22

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

Le théorème de Hua pour les algèbres artiniennes simples

H. Essannouni *, A. Kaidi

Département de Mathématiques & Informatique, Université Mohammed V, Faculté des Sciences, B.P. 1014, Rabat, Morocco

Received 15 February 1995; accepted 4 March 1999

Submitted by G.P. Barker

Abstract

Let D be a division ring and $M_n(D)$ be the ring of the $n \times n$ matrices with entries in D. Consider a surjective mapping $\sigma : M_n(D) \to M_n(D)$ satisfying $\sigma(A+B) = \sigma(A) + \sigma(B)$ for all $A, B \in M_n(D)$, $\sigma(1) = 1$ and for all invertible A in $M_n(D)$, $\sigma(A)$ is invertible and $\sigma(A^{-1}) = \sigma(A)^{-1}$. If $n = 1$ the well-known Hua's theorem states that σ is an automorphism or an anti-automorphism. We show that if $D \neq \mathbb{F}_2$ (the field of two elements) then σ is an automorphism or an anti-automorphism for all n. © 1999 Published by Elsevier Science Inc. All rights reserved.

AMS classification: 16A40

Keywords: Division ring; Automorphism; Anti-automorphism; Homomorphism of Jordan; Simple Artin algebra

1. Le théorème bien connu de Hua [5] affirme que si σ est une application bijective d'un anneau de division D dans D vérifiant $\sigma(a+b) = \sigma(a) + \sigma(b)$, $\sigma(1) = 1$ et $\sigma(a^{-1}) = \sigma(a)^{-1} (a \neq 0)$ alors σ est un automorphisme ou un anti-automorphisme. Ce résultat est utilisé en géométrie projective pour déterminer les transformations bijectives de la droite qui conservent les divisions harmoniques [2]. La démonstration est basée sur l'identité de Hua.

* Corresponding author.

PII: S0024-3795(99)00081-6

On peut vérifier directement que si x, y sont deux éléments inversibles d'un anneau R tels que $x - y^{-1}$ est aussi inversible, alors $x^{-1} - (x - y^{-1})^{-1}$ est inversible et on a

$$(x^{-1} - (x - y^{-1})^{-1})^{-1} = x - xyx. \tag{H}$$

Cette identité permet de montrer que σ est un homomorphisme de Jordan ($\sigma(aba) = \sigma(a)\sigma(b)\sigma(a)$ quels que soient $a, b \in D$). Ce qui constitue une étape importante dans la preuve du théorème de Hua.

Si au lieu d'un anneau de division D, on prend $\mathscr{U}$ une algèbre de dimension finie sur un corps infini ou une algèbre de Banach, alors en utilisant le calcul différentiel des applications rationnelles, comme dans [6], dans le premier cas et le calcul differentiel dans les espaces de Banach, comme dans [3], pour le deuxième, on peut établir que toute application σ de $\mathscr{U}$ dans $\mathscr{U}$ vérifiant:

(i) $\sigma(u + v) = \sigma(u) + \sigma(v)$ quels que soient $u, v \in \mathscr{U}$.

(ii) $\sigma(1) = 1$.

(iii) Pour tout u inversible dans $\mathscr{U}, \sigma(u)$ est aussi inversible et $\sigma(u^{-1}) = \sigma(u)^{-1}$.

est un homomorphisme de Jordan. Si on suppose de plus σ surjective et $\mathscr{U}$ première alors le théorème de Herstein [4] permet de conclure que σ est un homomorphisme ou un anti-homomorphisme.

Dans ce papier, nous nous interessons au cas où $\mathscr{U}$ est artinienne simple. D'après le théorème de Wedderburn–Artin, on peut supposer $\mathscr{U} = M_n(D)$ l'anneau des matrices carrées $n \times n$ à coefficients dans un anneau de division D. Nous montrons que si $D \neq \mathbb{F}_2$ ($\mathbb{F}_2$ le corps à deux éléments) alors σ est an automorphisme ou un anti-automorphisme.

Ce résultat n'est pas vrai en général, par exemple pour les algèbres suivantes: (1) $K[x]$ l'algèbre des polynômes à coefficients dans un corps K, (2) $A_n(K)$ la nième algèbre de Weyl avec $n \geqslant 1$ et K un corps de caractéristique zéro et (3) $\mathbb{H} \times \mathbb{H}$ où $\mathbb{H}$ est l'algèbre des quaternions réelle. En effect pour $K[x]$ et $A_n(K)$ les seuls éléments inversibles sont les éléments non nuls du corps de base et il est facile de construire des applications σ vérifiant (i)–(iii) qui ne sont ni des automorphismes ni des anti-automorphismes. Pour $\mathbb{H} \times \mathbb{H}$ soit $\sigma(x, y) = (x, \bar{y})$ où $\bar{y}$ est le conjugué de y, σ vérifie (i)–(iii) mais ce n'est ni un automorphisme, ni un anti-automorphisme. Notons que $K[x]$ est un domaine noetherien, $A_n(K)$ noethérienne simple et $\mathbb{H} \times \mathbb{H}$ est de dimension finie sur $\mathbb{R}$ en particulier elle est artinienne. Ces exemples montrent que le théorème de Hua ne peut pas s'étendre a des classes plus large que celle des algèbres artiniennes simples.

2. Dans toute la suite D est un anneau de division, $M_n(D)$ l'anneau des matrices carrées $n \times n$ à coefficients dans D et σ une application surjective de $M_n(D)$ dans $M_n(D)$ vérifiant:

(i) $\sigma(A + B) = \sigma(A) + \sigma(B)$ quels que soient $A, B \in M_n(D)$.

(ii) $\sigma(I) = I$, I étant la matrice unité.

(iii) Pour toute matrice inversible A de $M_n(D)$, $\sigma(A)$ est aussi inversible et $\sigma(A^{-1}) = \sigma(A)^{-1}$.

Notre but est de prouver.

Théorème A. *Si $D \neq \mathbb{F}_2$ alors σ est un automorphisme ou un anti-automorphisme.*

D'après le théorème de Herstein, il suffit de prouver que σ vérifie

$$\sigma(ABA) = \sigma(A)\sigma(B)\sigma(A)$$

quelles que soient les matrices $A, B \in M_n(D)$. Si $\mathrm{cara}(D) \neq 2$, c'est équivalent à montrer

$$\sigma(A^2) = \sigma(A)^2$$

quelle que soit $A \in M_n(D)$.

On considère $M_n(D)$ comme D-espace vectoriel à gauche et parfois on identifiera x avec xI pour $x \in D$. On désigne la matrice de $M_n(D)$ ayant 1 dans la position (i, j) et 0 ailleurs par E_{ij}. Toute matrice A de $M_n(D)$ s'écrit d'une manière unique sous la forme

$$A = \sum_{i,j} x_{ij} E_{ij}, \quad \text{où les } x_{ij} \in D.$$

Une matrice A de $M_n(D)$ est non-inversible si et seulement si il existe une matrice non nulle B telle que $AB = 0$ ce qui est encore équivalent à l'existence d'une matrice $X \in M_{n,1}(D), X \neq 0$, telle que $AX = 0$ ($M_{n,1}(D)$ étant l'ensemble des matrices ayant n lignes et une seule colonne à coefficients dans D).

Soit $A \in M_n(D)$ et soit Δ une partie de D, on pose

$$Sp_{\Delta}(A) = \{d \in \Delta \mid A - dI \text{ non-inversible}\}.$$

On a $d \in Sp_{\Delta}(A)$ si et seulement si il existe $X \in M_{n,1}(D), X \neq 0$, telle que $AX = dX$.

On notera la matrice de $M_{n,1}(D)$ ayant 1 dans la ième ligne et 0 ailleurs par E_i.

Lemme 2.1. (1) *Si $A = xE_{ij}$ alors $|Sp_D(A)| \leqslant 2$ où $|Sp_D(A)|$ est le cardinal de $Sp_D(A)$.*

(2) *Soit $A = xE_{ij} + yE_{k\ell}$ avec $x \neq 0, y \neq 0$ et $(i, j) \neq (k, \ell)$. Si $(k, \ell) \neq (j, i)$ alors $|Sp_D(A)| \leqslant 3$ et si $(k, \ell) = (j, i)$ alors les éléments non nuls d de $Sp_D(A)$ vérifient l'identité $dx^{-1}d = y$.*

Démonstration. Soit $A = x\,E_{ij}$ et soit $d \in Sp_D(A)$, alors il existe $X \in M_{n,1}(D)$, $X \neq 0$, tel que $AX = dX$. Posons $X = \sum_{k=1}^{n} a_k E_k$, on a $xa_j E_i = \sum_{k=1}^{n} da_k E_k$. Donc $da_i = xa_j$ et $da_k = 0$ pour $k \neq i$. Ainsi $Sp_D(A) = \{0\}$ si $i \neq j$ et $Sp_D(A) \subseteq \{0, x\}$ si $i = j$.

Soit maintenant $A = xE_{ij} + yE_{k\ell}$ avec $x \neq 0$, $y \neq 0$ et $(i,j) \neq (k,\ell)$. Supposons que $Sp_D(A)$ contient un élément non nul d. Soit $X \in M_{n,1}(D), X \neq 0$ tel que $AX = dX$. Posons $X = \sum_{r=1}^{n} a_r E_r$, on a $xa_j E_i + ya_\ell E_k = \sum_{r=1}^{n} da_r E_r$.

(1) $i = k$, alors $xa_j + ya_\ell = da_i$ et $a_r = 0$ pour $r \neq i$. Comme $X \neq 0$ alors $a_i \neq 0$ et par la suite $j = i$ ou $\ell = i$. Si $j = i$ et $\ell \neq i$ alors $d = x$ et si $j \neq i$ et $\ell = i$ alors $d = y$. Ainsi si $i = k$, $Sp_D(A)$ contient au plus un élément non nul.

(2) $i \neq k$, alors $xa_j = da_i$, $ya_\ell = da_k$ et $a_r = 0$ pour $r \neq i$ et $r \neq k$. Si $j \neq i$ et $j \neq k$ alors $a_i = 0$ donc $a_k \neq 0$ et par la suite $\ell = k$ ce qui donne $d = y$. Si $j = i$ et $a_i \neq 0$ alors $d = x$, si $j = i$ et $a_i = 0$ alors $a_k \neq 0$ et $\ell = k$ d'où $d = y$. Si $j = k$ alors $xa_k = da_i$, donc $a_i \neq 0$ et $a_k \neq 0$. Ainsi $\ell = k$ ou $\ell = i$, $\ell = k = j$ donne $d = y$, $\ell = i$ donne $ya_i = da_k$ et par la suite $ya_i = dx^{-1}da_i$ donc $dx^{-1}d = y$. □

Corollaire 2.2. *Si* $A = xE_{ij} + yE_{k\ell}$ *alors* $|Sp_{Z(D)}(A)| \leqslant 3$. $Z(D)$ *étant le centre de* D.

Proposition 2.3. *Si* $\mathrm{cara}(D) \neq 2,3$, σ *est un automorphisme ou un anti-automorphisme*.

Démonstration. D'après le théorème d'Herstein il suffit de prouver $\sigma(A^2) = \sigma(A)^2$, pour toute matrice $A \in M_n(D)$. Comme σ est additive, il suffit de le faire pour $A = xE_{ij} + yE_{k\ell}$. Soit F le sous-corps premier de D, $|F| \geqslant 5$. D'après le Corollaire 2.2. $|F - Sp_F(A)| \geqslant 2$. Soient $\alpha, \beta \in F - Sp_F(A)$ avec $\alpha \neq \beta$, posons $\gamma = (\beta - \alpha)^{-1}$. Les matrices $A - \alpha I$ et rI sont inversibles de même $(A - \alpha I) - (\gamma I)^{-1} = A - \beta I$ est aussi inversible. L'identité (H) avec $x = A - \alpha I$ et $y = \gamma I$ donne $\sigma(A^2) = \sigma(A)^2$. □

Le Théorème A est donc démontré dans le cas où la caractéristique de D est différente de 2 et de 3.

3. Cas où $\mathrm{cara}(D) = 3$. Dans cette section on suppose $\mathrm{cara}(D) = 3$.

Lemme 3.1. $\sigma(xAx) = \sigma(x)\sigma(A)\sigma(x)$ *quels que soient* $x \in D$ *et* $A \in M_n(D)$.

Démonstration. Il est facile de voir, en utilisant (H), que $\sigma(xyx) = \sigma(x)\sigma(y)\sigma(x)$ quels que soient $x, y \in D$. Soit $x \in D$ et $A \in M_n(D)$, on veut prouver

$$\sigma(xAx) = \sigma(x)\sigma(A)\sigma(x). \tag{3.1.1}$$

Comme σ est additive il suffit de prouver (3.1.1) pour $A = aE_{ij}$ avec $a \neq 0$.

(1) $i \neq j$. Alors $I + A$ est inversible et $(I + A)^{-1} = I - A$. On peut supposer $x \neq 0$ et $x \neq 1$. La matrice $xI - (I + A)^{-1}$ est inversible. L'identité (H) implique $\sigma(x(A + I)x) = \sigma(x)\sigma(A + I)\sigma(x)$ ce qui donne $\sigma(xAx) = \sigma(x)\sigma(A)\sigma(x)$.

(2) $i = j$. Supposons dans un premier temps $a \neq 1$ et $a \neq 2$. $I - A$ est inversible et $(I - A)^{-1} = I + ((1 - a)^{-1} - 1)E_{ii}$. On peut supposer $x \neq 0$ et $x \neq 1$.

La matrice $xI-(I-A)^{-1}$ est inversible si et seulement si $x \neq (1-a)^{-1}$. Donc si $x \neq (1-a)^{-1}$, (H) donne $\sigma(x(I-A)x) = \sigma(x)\sigma(I-A)\sigma(x)$ ce qui implique $\sigma(xAx) = \sigma(x)\sigma(A)\sigma(x)$. Si $x = (1-a)^{-1}$ alors $2I-A$ est inversible et $xI-(2I-A)^{-1}$ est aussi inversible. (H) donne

$$\sigma(x(2I-A)x) = \sigma(x)\sigma(2I-A)\sigma(x) \quad \text{d'où} \quad \sigma(xAx) = \sigma(x)\sigma(A)\sigma(x).$$

A présent prenons $a = 1$. On prend $x \neq 0$, $x \neq 1$ et $x \neq 2$. La matrice $I+A$ est inversible, aussi $xI-(I+A)^{-1}$ est inversible, et par la suite

$$\sigma(xAx) = \sigma(x)\sigma(A)\sigma(x). \quad \square$$

Corollaire 3.2. *$\sigma(xA+Ax) = \sigma(x)\sigma(A)+\sigma(A)\sigma(x)$ quels que soient $x \in D$ et $A \in M_n(D)$.*

Proposition 3.3. *Si* $\mathrm{cara}(D) = 3$ *alors σ est un automorphisme ou un anti-automorphisme.*

Démonstration. Il suffit de prouver $\sigma(A^2) = \sigma(A)^2$ pour $A = xE_{ij} + yE_{k\ell}$.

(1) $D \neq \mathbb{F}_3$ le corps à trois éléments. Nous affirmons qu'il existe $d \in D$ tel que $A-dI$ et $(A-dI)-I$ inversibles. Si $Z(D) \neq \mathbb{F}_3$ alors $|Z(D)| \geqslant 9$ est d'après le Corollaire 2.2, $|Sp_{Z(D)}(A)| \leqslant 3$, on peut donc choisir $d \in Z(D)$ tel que $d \notin Sp_{Z(D)}(A)$ et $1+d \notin Sp_{Z(D)}(A)$. Supposons $Z(D) = \mathbb{F}_3$. Si pour tout $d \in D$, $d \in Sp_D(A)$ ou $1+d \in Sp_D(A)$ alors d'aprés le Lemme 2.1, D vérifie une identité polynomiale généralisée. D'après [1] D doit être de dimension fini sur $Z(D)$ donc D est fini et par la suite commutatif. Ainsi $D = Z(D) = \mathbb{F}_3$, contradiction. Soit $d \in D$ tel que $A-dI$ et $(A-dI)-I$ inversibles. (H) donne $\sigma((A-dI)^2) = (\sigma(A-dI))^2$. Donc on a

$$\sigma(A^2) - \sigma(dA+Ad) + \sigma(d^2) = \sigma(A)^2 - \sigma(d)\sigma(A) - \sigma(A)\sigma(d) + \sigma(d)^2,$$

d'où $\sigma(A^2) = \sigma(A)^2$ d'après le Corollaire 3.2.

(2) $D = \mathbb{F}_3$. Il suffit de prouver

(a) $\sigma(E_{ij}^2) = \sigma(E_{ij})^2$ et (b) $\sigma((E_{ij}+E_{k\ell})^2) = (\sigma(E_{ij})+\sigma(E_{k\ell}))^2$ avec $(i,j) \neq (k,\ell)$

(a) Supposons $i \neq j$, alors $(I+E_{ij})^{-1} = I - E_{ij}$, donc $(I+\sigma(E_{ij}))(I-\sigma(E_{ij})) = I$ ce qui implique $\sigma(E_{ij})^2 = 0 = \sigma(E_{ij}^2)$. Si $i = j$ alors $(I+E_{ii})^2 = I$ donc $(\sigma(E_{ij})+I)^2 = I$ et par la suite $\sigma(E_{ii})^2 = \sigma(E_{ii}) = \sigma(E_{ii}^2)$.

(b) $A = E_{ij} + E_{k\ell}$ avec $(i,j) \neq (k,\ell)$.

(b.1) $i = k$.

(b.1.1) $i = j$, alors $(I+A)^2 = I$ donc $(I+\sigma(A))^2 = I$ d'où $\sigma(A^2) = \sigma(A) = \sigma(A)^2$.

(b.1.2) $i \neq j$ et $i = \ell$, aussi $\sigma(A)^2 = \sigma(A) = \sigma(A^2)$.

(b.1.3) $i \neq j$ et $i \neq l$ alors $A^2 = 0$. Donc $(I + A)(I - A) = I$ d'où $(I + \sigma(A))(I - \sigma(A)) = I$ et par la suite $\sigma(A)^2 = 0 = \sigma(A^2)$.

(b.2) $j = \ell$, similaire à (b.1).

(b.3) $i \neq k$ et $j \neq \ell$.

(b.3.1) $|\{i,k\} \cap \{j,\ell\}| = 0$ alors $\sigma(A^2) = 0 = \sigma(A)^2$.

(b.3.2) $|\{i,k\} \cap \{j,\ell\}| = 1$. Si $i = \ell$ alors $A^2 = E_{kj}$ et $A^3 = 0$. Donc $(I + A)^{-1} = (I + A)^2$. Ainsi $(I + \sigma(A))(I + 2\sigma(A) + \sigma(A^2)) = I$. Ce qui donne $\sigma(A)\sigma(A^2) = \sigma(A)^2 - \sigma(A^2)$. De même $\sigma(A^2)\sigma(A) = \sigma(A)^2 - \sigma(A^2)$. Donc $2(\sigma(A)^2 - \sigma(A^2)) = \sigma(A)\sigma(A^2) + \sigma(A^2)\sigma(A)$. Maintenant

$$\sigma(A)\sigma(A^2) + \sigma(A^2)\sigma(A) = \sigma(E_{ij})\sigma(E_{kj}) + \sigma(E_{kj})\sigma(E_{ij}) + \sigma(E_{ki})\sigma(E_{kj}) + \sigma(E_{kj})\sigma(E_{ki}).$$

Or $(E_{ij} + E_{kj})^2 = 0 = (E_{ki} + E_{kj})^2$ donc $(\sigma(E_{ij}) + \sigma(E_{kj}))^2 = 0 = (\sigma(E_{ki}) + \sigma(E_{kj}))^2$ et par la suite $2(\sigma(A)^2 - \sigma(A^2)) = \sigma(A)\sigma(A^2) + \sigma(A^2)\sigma(A) = 0$ donc $\sigma(A^2) = \sigma(A)^2$. Si $i = j$ alors $B^2 = B$ où $B = A + E_{kk}$, donc $\sigma(B^2) = \sigma(B)^2 = \sigma(B)$. Ce qui donne en tenant compte de ce qui précède $\sigma(E_{ii})\sigma(E_{k\ell}) + \sigma(E_{k\ell})\sigma(E_{ii}) + \sigma(E_{ii})\sigma(E_{kk}) + \sigma(E_{kk})\sigma(E_{ii}) = 0$. Posons $C = E_{ii} + E_{kk}$, on a $C^2 = C$ donc $\sigma(C^2) = \sigma(C) = \sigma(C)^2$. Ce qui donne $\sigma(E_{ii})\sigma(E_{kk}) + \sigma(E_{kk})\sigma(E_{ii}) = 0$ et par la suite $\sigma(E_{ii})\sigma(E_{k\ell}) + \sigma(E_{k\ell})\sigma(E_{ii}) = 0$.

A présent

$$\sigma(A)^2 = \sigma(E_{ii})^2 + \sigma(E_{ii})\sigma(E_{k\ell}) + \sigma(E_{k\ell})\sigma(E_{ii}) + \sigma(E_{k\ell})^2 = \sigma(E_{ii}) = \sigma(A^2).$$

De même si $k = \ell$ ou $k = j$, on trouve $\sigma(A^2) = \sigma(A)^2$.

(b.3.3) $|\{i,k\} \cap \{j,\ell\}| = 2$. si $i = j$ et $k = \ell$ alors $A^2 = A$ ce qui donne $\sigma(A^2) = \sigma(A) = \sigma(A)^2$. Supposons maintenant $i = \ell$ et $k = j$. Alors $A = E_{ij} + E_{ji}$ $(i \neq j)$. On a $(I + E_{ii} + E_{ij} + E_{ji})(l + E_{jj} - E_{ij} - E_{ji}) = I$ d'où

$$(I + \sigma(E_{ii}) + \sigma(E_{ij} + \sigma(E_{ji}))(I + \sigma(E_{jj}) - \sigma(E_{ij}) + \sigma(E_{ji})) = I,$$

$$(I + \sigma(E_{jj}) - \sigma(E_{ij}) - \sigma(E_{ji}))(I + \sigma(E_{ii}) + \sigma(E_{ij}) + \sigma(E_{ji})) = I$$

avec ces deux égalités et ce qui précède on obtient $\sigma(E_{ij})\sigma(E_{ji}) + \sigma(E_{ji})\sigma(E_{ij}) = \sigma(E_{ii}) + \sigma(E_{jj})$. Et par la suite

$$\sigma(A)^2 = \sigma(E_{ij})^2 + \sigma(E_{ji})^2 + \sigma(E_{ij})\sigma(E_{ji}) + \sigma(E_{ji})\sigma(E_{ij}) = \sigma(E_{ii}) + \sigma(E_{jj}) = \sigma(A^2). \quad \square$$

4. Cas où cara$(D) = 2$

Le lemme suivant est valable quelle que soit la caractéristique de D.

Lemme 4.1. *Si $A = xE_{ij} + yE_{k\ell} + zE_{rs}$ alors $|Sp_D(A)| \leqslant 4$ ou tous les éléments non nuls d de $Sp_D(A)$ vérifient une identité polynomiale généralisée de degré intérieur ou égal à* 3.

Démonstration. D'après le Lemme 2.1, on peut prendre $x \neq 0, y \neq 0, z \neq 0$ et les couples $(i,j);(k,\ell);(r,s)$ distincts deux à deux. Supposons que $Sp_D(A)$ contient un élément non nul d. Il existe $X \in M_{n,1}(D)$, $X \neq 0$, tel que $AX = dX$. Posons $X = \sum_{t=1}^{n} a_t E_t$, on a

$$xa_jE_i + ya_\ell E_k + za_sE_r = \sum_{t=1}^{n} da_tE_t.$$

(1) $i = k = r$. Alors $xa_j + ya_\ell + za_s = da_i$ et $a_t = 0$ pour $t \neq i$. Comme $X \neq 0$ alors $a_i \neq 0$ et par la suite $j = i$ ou $\ell = i$ ou $s = i$. Si $j = i$, $\ell \neq i$ et $s \neq i$ alors $d = x$, si $j \neq i$, $\ell = i$ et $s \neq i$ alors $d = y$ et si $j \neq i$, $\ell \neq i$ et $s = i$ alors $d = z$. Ainsi dans ce cas $|Sp_D(A)| \leqslant 2$.

(2) $i = k$ et $r \neq i$. Alors $xa_j + ya_\ell = da_i, za_s = da_r$ et $a_t = 0$ si $t \neq i, r$. Si $s \neq i$ et $s \neq r$ alors $a_r = 0$ et par la suite $j = i$ ou $\ell = i$, si $j = i$ et $\ell \neq i$ alors $d = x$ et si $j \neq i$ et $\ell = i$ alors $d = y$. Si $s = r$ alors $z = d$ ou $a_r = 0$. Supposons que $s = i$ alors $j \in \{i, r\}$ ou $\ell \in \{i, r\}$. Si $j = i$ et $\ell = r$ alors $xa_i + ya_r = da_i$ et par la suite $xz^{-1}\ da_r + ya_r = dz^{-1}\ da_r$ ce qui donne $xz^{-1}d + y = dz^{-1}d$. Si $j = i$ et $\ell \neq i, r$ alors $d = x$. Si $j = r$ et $\ell = i$ alors $xa_r + ya_i = da_i$ d'où $x + yz^{-1}d = dz^{-1}d$. Si $j = r$ et $\ell \neq i, r$ alors $xa_r = da_i$ ce qui donne $x = dz^{-1}d$. Si $j \neq i, r$ alors $\ell = i$ donne $d = y$ et $\ell = r$ donne $y = dz^{-1}d$.

(3) $i = r$ et $k \neq i$, similaire au (2).

(4) $k = r$ et $i \neq k$, similaire au (2).

(5) $i \neq k$, $i \neq r$ et $k \neq r$. Alors $xa_j = da_i$, $ya_\ell = da_k$, $za_s = da_r$ et $a_t = 0$ si $t \neq i, k, r$. Si $j \notin \{i, k, r\}$ alors $d \in Sp_D(yE_{k\ell} + zE_{rs})$. Donc on peut supposer j, ℓ et s des éléments de $\{i, k, r\}$. Si $j = i$ alors $d = x$ ou $d \in Sp_D(yE_{k\ell} + zE_{rs})$, de même $(\ell = k)$ et $(s = r)$ donnent des résultats analogues. Si $(j = k$ et $\ell = i)$ alors $y = dx^{-1}d$ ou $d \in Sp_D(zE_{rs})$, $(j = r, s = i)$ et $(\ell = r, s = k)$ sont similaires. Finalement $(j = k$, $\ell = r$ et $s = i)$ donne $z = dy^{-1}dx^{-1}d$ de même $(j = r$, $\ell = i$ et $s = k)$ donne un résultat analogue. □

Corollaire 4.2. *Si* $A = xE_{ij} + yE_{k\ell} + zE_{rs}$ *alors* $|Sp_{Z(D)}(A)| \leqslant 4$.

Dans toute la suite, on suppose cara$(D) = 2$.

Lemme 4.3. *Si* $|Z(D)| > 4$ *alors* $\sigma(\alpha^2 A) = \sigma(\alpha)\sigma(A)\sigma(\alpha)$ *quels que soit* $\alpha \in Z(D)$ *et* $A \in M_n(D)$.

Démonstration. On peut prendre $A = xE_{ij}$ et $\alpha \neq 0, 1$.

(1) $i \neq j$. $A + \alpha$ est inversible et $\alpha + (A + \alpha)^{-1}$ est inversible. L'identité (H) avec $x = \alpha$ et $y = A + \alpha$ donne

$$\sigma(\alpha(A + \alpha)\alpha) = \sigma(\alpha)\sigma(A + \alpha)\sigma(\alpha) \quad \Rightarrow \quad \sigma(\alpha^2 A) = \sigma(\alpha)\sigma(A)\sigma(\alpha).$$

(2) $i = j$. Comme $|Z(D)| > 4$, on peut choisir $\beta \in Z(D)$ tel que $\beta \neq 0$, $\beta \neq \alpha^{-1}, \beta \neq x$ et $\beta \neq \alpha + x$. Pour un tel β, $A + \beta$ est inversible ainsi que $\alpha + (A + \beta)^{-1}$.

$$(\mathrm{H}) \Rightarrow \sigma(\alpha(A + \beta)\alpha) = \sigma(\alpha)\sigma(A + \beta)\sigma(\alpha) \quad \Rightarrow \quad \sigma(\alpha^2 A) = \sigma(\alpha)\sigma(A)\sigma(\alpha).$$

Corollaire 4.4. *Si* $|Z(D)| > 4$ *alors*

$$(1)\quad \sigma(\alpha)\sigma(A) = \sigma(A)\sigma(\alpha), \quad (2)\quad \sigma(\alpha^2 A) = \sigma(\alpha^2)\sigma(A)$$

quels que soient $\alpha \in Z(D)$ *et* $A \in M_n(D)$.

Démonstration.

$$(1)\quad \sigma((\alpha+1)^2 A) = \sigma(\alpha+1)\sigma(A)\sigma(\alpha+1),$$

d'après le Lemme 4.3. Donc

$$\sigma(\alpha^2 A) + \sigma(A) = \sigma(\alpha)\sigma(A)\sigma(\alpha) + \sigma(A)\sigma(\alpha) + \sigma(\alpha)\sigma(A) + \sigma(A)$$
$$\Rightarrow \sigma(A)\sigma(\alpha) + \sigma(\alpha)\sigma(A) = 0 \Rightarrow \sigma(\alpha)\sigma(A) = \sigma(A)\sigma(\alpha).$$

$$(2)\quad \sigma(\alpha^2 A) = \sigma(\alpha)\sigma(A)\sigma(\alpha) = \sigma(\alpha^2)\sigma(A). \quad \square$$

Lemme 4.5. *Si* $|Z(D)| > 4$ *alors* $\sigma(A^2) = \sigma(A)^2$ *pour toute matrice* A *de* $M_n(D)$.

Démonstration. Comme σ est additive, il suffit de considérer A de la forme $A = xE_{ij} + yE_{k\ell}$. D'après le Corollaire 2.2, $|Sp_{Z(D)}(A)| \leqslant 3$. Comme $|Z(D)| \geqslant 5$, on peut choisir $\alpha^2,\ \beta^2 \in Z(D)$ tels que $\alpha^2 \neq \beta^2,\ \alpha^2 \notin Sp_{Z(D)}(A)$ et $\beta^2 \notin Sp_{Z(D)}(A)$. Posons $\gamma = (\alpha^2 + \beta^2)^{-1}$, les matrices $A + \alpha^2$ et $(A + \alpha^2) + \gamma^{-1}$ sont inversibles. L'identité (H) avec $x = A + \alpha^2$ et $y = \gamma$ donne

$$\sigma((A+\alpha)\gamma(A+\alpha)) = \sigma(A+\alpha)\sigma(\gamma)\sigma(A+\alpha)$$
$$\Rightarrow \sigma(\gamma A^2 + \gamma\alpha^2) = \sigma(\gamma)\sigma(A)^2 + \sigma(\gamma)\sigma(\alpha)^2 \quad \Rightarrow \quad \sigma(A^2) = \sigma(A)^2,$$

d'après le Corollaire 4.4. $\square$

Proposition 4.6. *Si* $|Z(D)| > 4$ *alors* α *est un automorphisme ou un anti-automorphisme.*

Démonstration. D'après le théorème de Herstein il suffit de prouver:

$$\sigma(ABA) = \sigma(A)\sigma(B)\sigma(A)$$

quelles que soient les matrices $A, B \in M_n(D)$. Comme σ est additive il suffit de considérer A de la forme $A = xE_{ij} + yE_{kl}$ et $B = zE_{rs}$.

(1) $r \neq s$. Posons $K = \{\alpha^2 \mid \alpha \in Z(D)\}$, K est un sous-corps de $Z(D)$ et $|K| \geqslant 8$. D'après les Corollaires 2.2 et 4.2, $|Sp_K(A)| \leqslant 3$ et $|Sp_K(A+B)| \leqslant 4$. On peut donc prendre $\alpha \in K$ tel que $\alpha \notin Sp_K(A)$ et $1 + \alpha \notin Sp_K(A+B)$. Pour un tel α, les matrices $A + \alpha$ et $(A+\alpha) + (B+1)^{-1}$ sont inversibles. (H) $\Rightarrow$ $\sigma((A+\alpha)(B+1)(A+\alpha)) = \sigma(A+\alpha)\sigma(B+1)\sigma(A+\alpha) \Rightarrow \sigma(ABA) = \sigma(A)\sigma(B)\sigma(A)$ d'après le Lemme 4.5.

(2) $r = s$. Soit $\gamma \in K$ avec $\gamma \neq 0$ et $\gamma \neq z$. La matrice $B + \gamma$ est inversible et $(B+\gamma)^{-1} = (\gamma^{-1} + (z+\gamma)^{-1})E_{rr} + \gamma^{-1}$. Posons $C = A + (\gamma^{-1} + (z+\gamma)^{-1})E_{rr}$. Il existe $\alpha \in K$ tel que $\alpha \notin Sp_K(A)$ et $\alpha + \gamma^{-1} \notin Sp_K(C)$. Pour un tel α, $A + \alpha$ et $A + \alpha - (B+\gamma)^{-1}$ sont inversibles.

$$(\mathrm{H}) \Rightarrow \sigma((A+\alpha)(B+\gamma)(A+\alpha)) = \sigma(A+\alpha)\sigma(B+\gamma)\sigma(A+\alpha)$$
$$\Rightarrow \sigma(ABA) = \sigma(A)\sigma(B)\sigma(A). \quad \square$$

Lemme 4.7. *Si D est non-commutatif alors $\sigma(A^2) = \sigma(A)^2$ pour toute matrice $A \in M_n(D)$.*

Démonstration. Il suffit de prendre $A = xE_{ij} + yE_{k\ell}$. Si $|Z(D)| > 4$ c'est déjà vu. Supposons que $|Z(D)| \leqslant 4$. Il existe $a \in D$ tel que $a \notin Sp_D(A)$ et $1 + a \notin Sp_D(A)$, car si non, d'après le Lemme 2.1, D satisfait une identité polynomiale généralisée et par la suite D est de dimension finie sur $Z(D)$ d'après [1]. Ainsi D est fini et par la suite commutatif, contradiction. Si on pose dans (H), $x = A + a$ et $y = 1$ puis on applique σ on obtient

$$\sigma((A+a)^2) = \sigma(A+a)^2$$
$$\Rightarrow \sigma(A^2) + \sigma(aA + Aa) = \sigma(A)^2 + \sigma(a)\sigma(A) + \sigma(A)\sigma(a).$$

Il existe aussi $b \in D$ tel que

$$b \notin Sp_D(A),\ \ 1 + b \notin Sp_D(A),\ \ a + b \notin Sp_D(A) \ \text{ et } \ a + b + 1 \notin Sp_D(A).$$

D'après ce qui précède

$$\sigma(A^2) + \sigma(A)^2 = \sigma((a+b)A + A(a+b)) + \sigma(a+b)\sigma(A) + \sigma(A)\sigma(a+b)$$
$$= \sigma(aA + Aa) + \sigma(bA + Ab) + \sigma(a)\sigma(A) + \sigma(A)\sigma(a) + \sigma(b)\sigma(A)$$
$$+ \sigma(A)\sigma(b) = 0$$
$$\Rightarrow \sigma(A^2) = \sigma(A)^2. \quad \square$$

Lemme 4.8. *Si D est non-commutatif alors $\sigma(aAa) = \sigma(a)\sigma(A)\sigma(a)$ quels que soient $a \in D$ et $A \in M_n(D)$.*

Démonstration. On peut supposer $A = xE_{ij}$ et $a \neq 0$.

(1) $i \neq j$. Soit $b \in D$ tel que $b \neq 0$ et $b \neq a^{-1}$. La matrice $A + b$ est inversible et $a + (A+b)^{-1}$ est aussi inversible. Donc

$$\sigma(a(A+b)a) = \sigma(a)\sigma(A+b)\sigma(a) \quad \Rightarrow \quad \sigma(aAa) = \sigma(a)\sigma(A)\sigma(b).$$

(2) $i = j$. Soit $b \in D$ tel que $b \neq 0$, $b \neq x$, $b \neq a^{-1}$ et $b \neq x + a^{-1}$. Alors $A + b$ est inversible et $a + (A+b)^{-1}$ est inversible, d'où

$$\sigma(a(A+b)a) = \sigma(a)\sigma(A+b)\sigma(a) \quad \Rightarrow \quad \sigma(aAa) = \sigma(a)\sigma(A)\sigma(a). \quad \square$$

Lemme 4.9. *Si D est non-commutatif alors*
(1) $\sigma(Aa^2A) = \sigma(A)\sigma(a)^2\sigma(A)$.
(2) $\sigma(Ab^2a + ab^2A) = \sigma(A)\sigma(b)^2\sigma(a) + \sigma(a)\sigma(b)^2\sigma(A)$.
(3) $\sigma(ABa^2 + a^2BA) = \sigma(A)\sigma(B)\sigma(a)^2 + \sigma(a)^2\sigma(B)\sigma(A)$ *quels que soient* $a, b \in D$ *et* $A, B \in M_n(D)$.

Démonstration. (1) D'après les Lemmes 4.7 et 4.8,

$$\sigma((aAa)^2) = \sigma(aAa)^2 = (\sigma(a)\sigma(A)\sigma(a))^2 = \sigma(a)\sigma(A)\sigma(a^2)\sigma(A)\sigma(a).$$

Et $\sigma((aAa)^2) = \sigma(aAa^2Aa) = \sigma(a)\sigma(Aa^2A)\sigma(a)$. D'où $\sigma(Aa^2A) = \sigma(A)\sigma(a)^2\sigma(A)$.

(2) $\sigma((A+a)b^2(A+a)) = \sigma(A+a)\sigma(b^2)\sigma(A+a)$

$$\Rightarrow \sigma(Ab^2a + ab^2A) = \sigma(A)\sigma(b)^2\sigma(a) + \sigma(a)\sigma(b)^2\sigma(A).$$

(3) $\sigma((A+B)a^2(A+B)) = \sigma(A+B)\sigma(a)^2\sigma(A+B)$

$$\Rightarrow \sigma(Aa^2B + Ba^2A) = \sigma(A)\sigma(a)^2\sigma(B) + \sigma(B)\sigma(a)^2\sigma(A).$$

A présent

$$\begin{aligned}
\sigma(ABa^2 + a^2BA) &= \sigma(A(Ba^2 + a^2B) + Aa^2B + (a^2B + Ba^2)A + Ba^2A) \\
&= \sigma(A(Ba^2 + a^2B) + (Ba^2 + a^2B)A) + \sigma(Aa^2B + Ba^2A) \\
&= \sigma(A)\sigma(Ba^2 + a^2B) + \sigma(Ba^2 + a^2B)\sigma(A) + \sigma(A)\sigma(a)^2\sigma(B) \\
&\quad + \sigma(B)\sigma(a)^2\sigma(A) \\
&= \sigma(A)[\sigma(B)\sigma(a^2) + \sigma(a^2)\sigma(B)] + [\sigma(B)\sigma(a^2) + \sigma(a^2)\sigma(B)]\sigma(A) \\
&\quad + \sigma(A)\sigma(a)^2\sigma(B) + \sigma(B)\sigma(a)^2\sigma(A) \\
&= \sigma(A)\sigma(B)\sigma(a)^2 + \sigma(a)^2\sigma(B)\sigma(A). \quad \square
\end{aligned}$$

Proposition 4.10. *Si D est non-commutatif alors σ est un automorphisme ou un anti-automorphisme.*

Démonstration. On peut supposer $|Z(D)| \leqslant 4$. On doit prouver que:

$$\sigma(ABA) = \sigma(A)\sigma(B)\sigma(A)$$

quelles que soient les matrices $A, B \in M_n(D)$. Comme σ est additive il suffit de prendre $A = xE_{ij} + yE_{k\ell}$ et $B = zE_{rs}$.

(1) $r \neq s$. On peut choisir $a \in D$ tel que $a^2 \notin Sp_D(A)$ et $1 + a^2 \notin Sp_D(A+B)$, car si non, d'après les Lemmes 2.1 et 4.1, D satisfait une identité polynomiale généralisée, d'après [1] D doit être de dimension finie sur $Z(D)$ et par la suite D est fini donc commutatif, contradiction. Pour un tel $a, A + a^2$ est inversible et

$A + a^2 + (B+1)^{-1} = A + B + 1 + a^2$ est aussi inversible. Si on pose dans l'identité (H) $x = A + a^2$ et $y = B + 1$, puis on applique σ, on obtient:

$$\begin{aligned}
&\sigma((A+a^2)(B+1)(A+a^2)) = \sigma(A+a^2)\sigma(B+1)\sigma(A+a^2)\\
&\quad\Rightarrow \sigma(ABA) + \sigma(ABa^2 + a^2BA) + \sigma(A^2) + \sigma(Aa^2 + a^2A) + \sigma(a^4)\\
&\qquad = \sigma(A)\sigma(B)\sigma(A) + \sigma(A)\sigma(B)\sigma(a)^2 + \sigma(a)^2\sigma(B)\sigma(A) + \sigma(A)^2\\
&\qquad\quad + \sigma(A)\sigma(a)^2 + \sigma(a)^2\sigma(A) + \sigma(a)^4\\
&\quad\Rightarrow \sigma(ABA) = \sigma(A)\sigma(B)\sigma(A)
\end{aligned}$$

d'après les Lemmes 4.7 et 4.9.

(2) $r = s$. Soit $b \in D$ avec $b \neq 0$ et $b^2 \neq z$. La matrice $B + b^2$ est inversible et on a:

$$(B+b^2)^{-1} = ((z+b^2)^{-1} + b^{-2})E_{rr} + b^{-2}.$$

Posons $C = A + ((z+b^2)^{-1} + b^{-2})E_{rr}$. On peut choisir $a \in D$ tel que $a^2 \notin Sp_D(A)$ et $a^2 + b^{-2} \notin Sp_D(C)$. Pour un tel a, $A + a^2$ est inversible et $(A+a^2) + (B+b^2)^{-1}$ est inversible. Donc

$$\begin{aligned}
&\sigma((A+a^2)(B+b^2)(A+a^2)) = \sigma(A+a^2)\sigma(B+b^2)\sigma(A+a^2)\\
&\quad\Rightarrow \sigma(ABA) + \sigma(ABa^2 + a^2BA) + \sigma(Ab^2A) + \sigma(Ab^2a^2 + a^2b^2A)\\
&\qquad + \sigma(a^2Ba^2) + \sigma(a^2b^2a^2)\\
&\qquad = \sigma(A)\sigma(B)\sigma(A) + \sigma(A)\sigma(B)\sigma(a^2) + \sigma(a^2)\sigma(B)\sigma(A)\\
&\qquad\quad + \sigma(A)\sigma(b^2)\sigma(A) + \sigma(A)\sigma(b^2)\sigma(a^2) + \sigma(a^2)\sigma(b^2)\sigma(A)\\
&\qquad\quad + \sigma(a^2)\sigma(B)\sigma(a^2) + \sigma(a^2)\sigma(b^2)\sigma(a^2)\\
&\quad\Rightarrow \sigma(ABA) = \sigma(A)\sigma(B)\sigma(A),
\end{aligned}$$

d'après les Lemmes 4.8 et 4.9. □

Pour terminer la démonstration du Théorème A, il nous reste à regarder le cas où $D = \mathbb{F}_4$ le corps à quatre éléments. On pose $\mathbb{F}_4 = \{0, 1, \omega, 1+\omega\}$ avec $\omega^2 = 1 + \omega$. Tout élément de $\mathbb{F}_4$ est un carré.

Lemme 4.11. *Pour toute matrice A de $M_n(\mathbb{F}_4)$ et pour tout $\alpha \in \mathbb{F}_4$ on a*:

$$\sigma(\alpha A\alpha) = \sigma(\alpha)\sigma(A)\sigma(\alpha).$$

Démonstration. On peut prendre $A = xE_{ij}$ avec $0 \neq x \in \mathbb{F}_4$ et $\alpha \neq 0, 1$.

(1) $i \neq j$. $A + 1$ est inversible et $\alpha + (A+1)^{-1}$ est aussi inversible. Donc $\sigma(\alpha(A+1)\alpha) = \sigma(\alpha)\sigma(A+1)\sigma(\alpha) \Rightarrow \sigma(\alpha A\alpha) = \sigma(\alpha)\sigma(A)\sigma(\alpha)$.

(2) $i = j$. Si $x = \alpha^{-1}$ alors $A + \alpha$ est inversible et $\alpha + (A + \alpha)^{-1}$ inversible. Donc $\sigma(\alpha(A + \alpha)\alpha) = \sigma(\alpha)\sigma(A + \alpha)\sigma(\alpha) \Rightarrow \sigma(\alpha A\alpha) = \sigma(\alpha)\sigma(A)\sigma(\alpha)$. Soit maintenant $x \in \{1, \alpha\}$. Supposons dans un premier temps n impair et soit $m = \frac{n+1}{2}$. Considérons la matrice $M = \sum_{k=1}^{n} E_{k,n+1-k}$, on a $M^2 = I$. Comme $\alpha + (xM)^{-1}$ est inversible alors

$$\sigma(\alpha(xM)\alpha) = \sigma(\alpha)\sigma(xM)\sigma(\alpha) \quad \Rightarrow \quad \sigma(\alpha(xE_{m,m})\alpha) = \sigma(\alpha)\sigma(xE_{mm})\sigma(\alpha).$$

Pour $i \neq m$, posons $N = E_{ii} + \alpha M$ et $R = \alpha E_{ii} + M$. Les matrices N et R sont inversibles ainsi que $\alpha + N^{-1}, \alpha + R^{-1}, \alpha + M^{-1}$ et $\alpha + (\alpha M)^{-1}$ sont aussi inversibles. Donc $\sigma(\alpha N\alpha) = \sigma(\alpha)\sigma(N)\sigma(\alpha)$ et $\sigma(\alpha R\alpha) = \sigma(\alpha)\sigma(R)\sigma(\alpha)$ ce qui donne $\sigma(\alpha(xE_{ii})\alpha) = \sigma(\alpha)\sigma(xE_{ii})\sigma(\alpha)$ pour $x \in \{1, \alpha)$. A présent supposons que n est pait et soit $M = \sum_{k=1}^{n} E_{k,n+1-k}$, $N = E_{ii} + \alpha M$ et $R = \alpha E_{ii} + M$, on a $M^2 = I, N$ et R inversibles ainsi que $\alpha + N^{-1}$, $\alpha + R^{-1}$, $\alpha + M^{-1}$ et $\alpha + (\alpha M)^{-1}$. Ce qui donne comme avant $\sigma(\alpha(xE_{ii})\alpha) = \sigma(\alpha)\sigma(xE_{ii})\sigma(\alpha)$ pour $x \in \{1, \alpha\}$. □

Corollaire 4.12. *$\sigma(\alpha A) = \sigma(\alpha)\sigma(A) = \sigma(A)\sigma(\alpha)$ pour toute matrice $A \in M_n(\mathbb{F}_4)$ et tout $\alpha \in \mathbb{F}_4$.*

Démonstration.

$$\begin{aligned}
&\sigma((1 + \alpha)^2 A) = \sigma(1 + \alpha)\sigma(A)\sigma(1 + \alpha)\\
&\quad \Rightarrow \sigma(A) + \sigma(\alpha^2 A) = \sigma(A) + \sigma(\alpha)\sigma(A) + \sigma(A)\sigma(\alpha) + \sigma(\alpha)\sigma(A)\sigma(\alpha)\\
&\quad \Rightarrow \sigma(\alpha)\sigma(A) + \sigma(A)\sigma(\alpha) = 0 \Rightarrow \sigma(\alpha)\sigma(A) = \sigma(A)\sigma(\alpha).
\end{aligned}$$

A présent soit $\alpha \in \mathbb{F}_4$ il existe $\beta \in \mathbb{F}_4$ tel que $\alpha = \beta^2$. On a

$$\sigma(\alpha A) = \sigma(\beta^2 A) = \sigma(\beta)\sigma(A)\sigma(\beta) = \sigma(\beta^2)\sigma(A) = \sigma(\alpha)\sigma(A). \quad \square$$

Lemme 4.13. *$\sigma(A^2) = \sigma(A)^2$ pour toute matrice A de $M_n(\mathbb{F}_4)$.*

Démonstration. Comme σ est additive, il suffit de prendre $A = xE_{ij} + yE_{k\ell}$ avec $x, y \in \mathbb{F}_4$. Et d'après le Lemme 4.12 il suffit de prendre $A = E_{ij}$ et $A = E_{ij} + E_{k\ell}$ avec $(i, j) \neq (k, \ell)$.

(1) $A = E_{ij}$. Supposons $i \neq j$ alors $A^2 = 0$. Donc

$$(1 + A)^2 = 1 \;\Rightarrow\; (1 + \sigma(A))^2 = 1 \;\Rightarrow\; \sigma(A)^2 = 0 = \sigma(A^2).$$

Supposons $i = j$. Alors $A + \omega$ et $A + \omega + 1$ sont inversibles donc $\sigma((A + \omega)^2) = \sigma(A + \omega)^2 \Rightarrow \sigma(A^2) = \sigma(A)^2$.

(2) $A = E_{ij} + E_{k\ell}$ avec $(i, j) \neq (k, \ell)$. D'après le Lemme 2.1, $Sp_{\mathbb{F}_4}(A) \subseteq \{0, 1\}$. Considérons $\alpha, \beta \in \mathbb{F}_4$ tels que $\alpha \neq \beta$, $\alpha \notin Sp_{\mathbb{F}_4}(A)$ et $\beta \notin Sp_{\mathbb{F}_4}(A)$. Posons $\gamma = (\alpha + \beta)^{-1}$, les matrices $A + \alpha$ et $(A + \alpha) + \gamma^{-1}$ sont inversibles.

$$(\mathrm{H}) \Rightarrow \sigma((A + \alpha)\gamma(A + \alpha)) = \sigma(A + \alpha)\sigma(\gamma)\sigma(A + \alpha) \Rightarrow \sigma(A^2) = \sigma(A)^2. \quad \square$$

Proposition 4.14. *Si $D = \mathbb{F}_4$ alors σ est un automorphisme ou un anti-automorphisme.*

Démonstration. D'après le théorème de Herstein il suffit de montrer

$$\sigma(ABA) = \sigma(A)\sigma(B)\sigma(A)$$

où A et B sont arbitraires dans $M_n(\mathbb{F}_4)$. Comme σ est additive, il suffit de le prouver pour $A = xE_{ij} + yE_{k\ell}$ et $B = zE_{rs}, x, y, z \in \mathbb{F}_4$.

(1) $A = xE_{ij}$ et $B = zE_{rs}$. On peut prendre $A = E_{ij}$ et $B = E_{rs}$. Supposons $r \neq s$ alors $B+1$ est inversible et $(B+1)^{-1} = B+1$. Les matrices $A+\omega$ et $(A+\omega)+(B+1)^{-1}$ sont inversibles donc

$$\sigma((A+\omega)(B+1)(A+\omega)) = \sigma(A+\omega)\sigma(B+1)\sigma(A+\omega)$$
$$\Rightarrow \sigma(ABA) = \sigma(A)\sigma(B)\sigma(A).$$

Supposons $r = s$ et $i \neq j$, $E_{rr} + \omega$ est inversible de même $(E_{ij}+1)+(E_{rr}+\omega)^{-1}$. Donc

$$\sigma((E_{ij}+1)(E_{rr}+\omega)(E_{ij}+1)) = \sigma(E_{ij}+1)\sigma(E_{rr}+\omega)\sigma(E_{ij}+1)$$
$$\Rightarrow \sigma(E_{ij}E_{rr}E_{ij}) = \sigma(E_{ij})\sigma(E_{rr})\sigma(E_{ij}).$$

Supposons finalement $r = s$ et $i = j$. Si $i = r$ alors

$$\sigma(ABA) = \sigma(E_{ii}^3) = \sigma(E_{ii}^2) = \sigma(E_{ii})^2 = \sigma(E_{ii}) = \sigma(E_{ii})^3.$$

Pour $i \neq r$, posons $C = (1+\omega)E_{rr}$. Les matrices $A+\omega$ et $C+1$ sont inversibles de même $A+\omega+(C+1)^{-1}$ est aussi inversible. Ainsi

$$\sigma((E_{ii}+\omega)(C+1)(E_{ii}+\omega)) = \sigma(E_{ii}+\omega)\sigma(C+1)\sigma(E_{ii}+\omega)$$
$$\Rightarrow \sigma(E_{ii}E_{rr}E_{ii}) = \sigma(E_{ii})\sigma(E_{rr})\sigma(E_{ii}).$$

(2) $A = E_{ij} + E_{k\ell}$ et $B = E_{rs}$. Considérons d'abord le cas $r \neq s$. Posons $C = zE_{rs}$, $C+1$ est inversible. Comme $Sp_{\mathbb{F}_4}(A) \subseteq \{o, 1\}$ alors $A+\omega$ est inversible. Posons $M = (A+\omega)+(C+1)^{-1} = E_{ij} + E_{k\ell} + zE_{rs} + 1 + \omega$. En examinant $Sp_{\mathbb{F}_4}(E_{ij} + E_{k\ell} + zE_{rs})$, on peut toujours choisir $z \neq 0$ de telle sorte que M soit inversible (voir la démonstration du Lemme 4.1). Pour un tel z

$$\sigma((A+\omega)(zE_{rs}+1)(A+\omega)) = \sigma(A+\omega)\sigma(zE_{rs}+1)\sigma(A+\omega)$$
$$\Rightarrow \sigma(ABA) = \sigma(A)\sigma(B)\sigma(A).$$

Supposons maintenant $r = s$. La matrice $\omega E_{rr} + 1$ est inversible et $(\omega E_{rr}+1)^{-1} = 1 + (1+\omega)E_{rr}$. Si $z \neq 0, 1$, $z \in \mathbb{F}_4$, alors $A+z$ est inversible. Posons $N = (A+z)+(1+\omega E_{rr})^{-1} = E_{ij} + E_{k\ell} + (1+\omega)E_{rr} + 1 + z$. Aussi on peut toujours choisir $z \in \{\omega, 1+\omega\}$ de telle sorte que N soit inversible. Ce qui donne comme avant $\sigma(ABA) = \sigma(A)\sigma(B)\sigma(A)$. □

Remarque 4.15. Pour $D = \mathbb{F}_2$, on ne dispose pas de contre exemples. Nous pensons que le Théorème A est vrai même dans ce cas. En particulier il est vrai si $n = 2$.

Proposition 4.16. *Si $D = \mathbb{F}_2$ et $n = 2$ alors σ est un automorphisme ou un anti-automorphisme.*

Démonstration. Les matrices inversibles de $M_2(\mathbb{F}_2)$ sont

$$I,\quad A_1=\begin{bmatrix}1&1\\1&0\end{bmatrix},\quad A_2=\begin{bmatrix}1&0\\1&1\end{bmatrix},\quad A_3=\begin{bmatrix}1&1\\0&1\end{bmatrix},$$
$$A_4=\begin{bmatrix}0&1\\1&0\end{bmatrix}\quad\text{et}\quad A_5=\begin{bmatrix}0&1\\1&1\end{bmatrix}$$

avec $A_1^{-1}=A_5$ et $A_i^{-1}=A_i$ pour $i=2,3,4$. Les matrices I,A_1,A_2 et A_3 sont $\mathbb{F}_2$ linéairement indépendantes, donc forment une base de $M_2(\mathbb{F}_2)$. Posons

$$\sigma(A_1)=\begin{bmatrix}a&b\\c&d\end{bmatrix},\quad \sigma(A_2)=\begin{bmatrix}\alpha&\beta\\\gamma&\delta\end{bmatrix}\quad\text{et}\quad \sigma(A_3)=\begin{bmatrix}\alpha'&\beta'\\\gamma'&\delta'\end{bmatrix},$$

- $\sigma(A_1^{-1})=\sigma(A_1)^{-1}$ donne $\sigma(A_1)=\begin{bmatrix}a&1\\1&1+a\end{bmatrix}$ où $a\in\mathbb{F}_2$,
- $\sigma(A_2^{-1})=\sigma(A_2)^{-1}$ donne $\sigma(A_2)=\begin{bmatrix}\alpha&\beta\\\gamma&\alpha\end{bmatrix}$ avec $\beta\gamma=1+\alpha$,
- $\sigma(A_3^{-1})=\sigma(A_3)^{-1}$ donne $\sigma(A_3)=\begin{bmatrix}\alpha'&\beta'\\\gamma'&\alpha'\end{bmatrix}$ avec $\beta'\gamma'=1+\alpha'$.
- Finalement $\sigma(A_4^{-1})=\sigma(A_4)^{-1}$ donne $\beta\gamma'+\beta'\gamma=1$.

Donc on a le système

$$(\delta)\begin{cases}\beta\gamma=1+\alpha\\ \beta'\gamma'=1+\alpha'\\ \beta\gamma'+\beta'\gamma=1\end{cases}$$

(S) possède 6 solutions qui sont:

$$(\alpha,\beta,\gamma,\alpha',\beta',\gamma')=(0,1,1,1,1,0);(0,1,1,1,0,1);(1,0,1,0,1,1);$$
$$(1,0,1,1,1,0);(1,1,0,0,1,1)\text{ ou }(1,1,0,1,0,1).$$

D'autre part on a 2 chois possibles pour a. Ainsi le nombre des σ possibles est 12. Or 12 est exactement le nombre total des automorphismes et des anti-automorphismes de $M_2(\mathbb{F}_2)$. □

References

[1] S.A. Amitsur, Generalized polynomial identities and pivotal monomials, Trans. Am. Math. Soc. 114 (1965) 210–226.
[2] E. Artin, Geometric Algebra, Interscience, New York, 1957.
[3] H. Essannouni, A. Kaidi, H-Structures de Banach, preprint, Université Mohammed V, Rabat 1989.
[4] I.N. Herstein, Topics in Ring Theory, University of Chicago Press, Chicago, 1969.
[5] L.K. Hua, On the automorphisms of field, Proc. Nat. Acad. Sci. USA 35 (1949) 386–389.
[6] K. Mccrimmon, Axioms for inversion in Jordan algebras, J. Algebra 47 (1977) 201–222.